UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/698,784	10/31/2003	John Apostolopoulos	200312858-1	1717

22879 7590 02/02/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
KOEMPEL THOMAS, BEATRICE L	
ART UNIT	PAPER NUMBER
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/698,784	APOSTOLOPOULOS ET AL.	
	Examiner	Art Unit	
	Bea Koempel-Thomas	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *2 February 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *21 June 2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-34 are pending in this application and presented for examination.

Objections

Abstract

1. Applicant is reminded of the proper language and format for an abstract of the disclosure. The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details. The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

2. The abstract should include the following:

   a. for a machine or apparatus, its organization and operation;

   b. for a process, the steps.

Extensive mechanical and design details of apparatus should not be given.

3. The abstract of the disclosure is objected to because it includes phrases that can be implied, “Disclosed are,” and ”the present invention.” The abstract of the disclosure is further objected to because it includes the legal phraseology “in one embodiment.” Each phrase is

objected to as not necessary for a concise statement of the technical disclosure of the patent. Further, the abstract should include that which is new in the art to which the invention pertains regarding the claimed methods, apparatuses, and article of manufacture. Appropriate correction is required. See MPEP § 608.01(b).

Drawings

4. Figures 1A-1C should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claim 14 and all claims dependent thereon are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 14 could reasonably be drawn to non-functional descriptive material, per se, i.e., *instructions stored therein* may be taken to mean a program listing recorded on a computer-readable storage medium without any

functional interrelationship, and as such, claim 14, would be directed to non-statutory subject matter. The specification does not preclude this interpretation. Further, claim 14 does not necessarily transform a physical object to a different state or thing nor produce a useful, concrete and tangible result.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 28 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The clause of claim 28 beginning on line 4 of the claim: "said first segment, and said cryptographic checksum for said first of said plurality of data segments," renders the invention to which claim 28 was intended to be directed unclear, making claim 28 indefinite.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. **Claims 1, 2, 5-10, 12, 13, 23-30, and 32-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wee et al., "Secure Scalable Video Streaming for Wireless Networks," IEEE International Conference on Acoustics, Speech, and Signal Processing, Salt Lake City, Utah, May 2001, (hereinafter Wee) in view of Miller et al., U.S. Patent No. 5,790,669 (hereinafter Miller).**

11. **Regarding claim 1:** Wee discloses a method (page 1 col. 2 ¶2) for ensuring the integrity of data, comprising: for a plurality of data packets comprising a plurality of first data segments and a plurality of second data segments (page 3 col. 1 ¶2).

Wee does not disclose calculating a cryptographic checksum for said plurality of said first data segments; or enabling said cryptographic checksum for said plurality of said first data segments to be transmitted separately from said plurality of data packets.

Miller discloses calculating a cryptographic checksum for said plurality of said first data segments (col. 1 lines 27-44); and enabling said cryptographic checksum for said plurality of said first data segments to be transmitted separately from said plurality of data packets (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

12. **Regarding claim 2:** Wee discloses a plurality of said second data segments (page 3 col. 1 ¶2).

Wee does not disclose calculating a cryptographic checksum; and enabling said cryptographic checksum for said plurality of said second data segments to be transmitted separately from said plurality of data packets.

Miller discloses calculating a cryptographic checksum (col. 1 lines 27-44); and enabling said cryptographic checksum for said plurality of said second data segments to be transmitted separately from said plurality of data packets (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

13. **Regarding claim 5:** Wee discloses an opportunistic integrity checking scheme (page 1 col. 1 ¶3).

14. **Regarding claim 6:** Wee does not disclose that said calculating of said cryptographic checksum is performed using a technique selected from the group consisting of: a hash function providing a fingerprint of data contained in an encrypted data packet and which guarantees the authenticity of received data and the validity of decrypted data, Message Authentication Codes (MAC), Message Digest algorithms, keyed hashes, SHA (Secure Hash Algorithm), RIPEMD (RACE Integrity Primitives Evaluation Message Digest), HMAC (keyed-Hashing for Message Authentication), and digital signature schemes.

Miller discloses that said calculating of said cryptographic checksum is performed using the techniques of: a hash function providing a fingerprint of data contained in an encrypted data

packet and which guarantees the authenticity of received data and the validity of decrypted data (col. 7 lines 40-44), and digital signature schemes (col. 1-2 lines 60-4).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

15. **Regarding claim 7:** Wee discloses that said plurality of said data packets comprises secure scalably streamable data (Title).

16. **Regarding claim 8:** Wee discloses that said plurality of said data packets include data comprising scalably compressed data for media selected from the group consisting of: speech, audio, image (*see* 5.1: Scalable Coding – Packetization), video (page 1 col. 1 ¶2), and computer graphics.

17. **Regarding claim 9:** Wee discloses that said plurality of said data packets include data scalably formatted according to the techniques of: JPEG-2000 (page 2 col. 1 ¶5) with spatial scalability (page 3 col. 1 ¶1 and ¶3); MPEG-1/2/4 (page 2 col. 1 ¶5) or H.261/2/3/4 (page 2 col. 1 ¶5) using spatial scalability (page 3 col. 1 ¶1 and ¶3); and progressive/scalable graphics compression (page 3 §5.1).

18. **Regarding claim 10:** Wee discloses that said plurality of said data packets comprises media data (page 3 col. 1 ¶2).

19. **Regarding claim 12:** Wee discloses encrypting one or more data packets (pages 3-4 §5.2).

20. **Regarding claim 13:** Wee and Miller disclose said cryptographic checksum as indicated regarding claim 1, above. Wee further discloses encrypting (pages 3-4 §5.2).

21. **Regarding claim 23:** Wee discloses an apparatus for ensuring integrity of data, comprising:

a receiver for receiving a plurality of data packets each of said packets comprising one or more data segments (page 1 col. 1 ¶2).

Wee does not disclose a cryptographic checksum calculator coupled to said receiver, said cryptographic checksum calculator for calculating a cryptographic checksum for one or more of said data segments; or a cryptographic checksum appender coupled to said cryptographic checksum calculator for assembling said cryptographic checksum.

Miller discloses a cryptographic checksum calculator coupled to said receiver, said cryptographic checksum calculator for calculating a cryptographic checksum for one or more of said data segments (col. 1 lines 27-44); and a cryptographic checksum appender coupled to said cryptographic checksum calculator for assembling said cryptographic checksum (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

22. **Regarding claim 24:** Wee discloses a plurality of data packets comprising a plurality of first data segments and a plurality of second data segments (page 3 col. 1 ¶2).

Wee does not disclose that said cryptographic checksum calculator is enabled to calculate a cryptographic checksum for said plurality of said first data segments; or to enable said cryptographic checksum for said plurality of said first data segments to be transmitted separately from said plurality of data packets.

Miller discloses that said cryptographic checksum calculator is enabled to calculate a cryptographic checksum for said plurality of said first data segments (col. 1 lines 27-44); and to enable said cryptographic checksum for said plurality of said first data segments to be transmitted separately from said plurality of data packets (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

23. **Regarding claim 25:** Wee does not disclose that said cryptographic checksum calculator is enabled to calculate said cryptographic checksum for said set of said data segments independently of cryptographic checksums calculated for other sets of said data segments.

Miller discloses that said cryptographic checksum calculator is enabled to calculate said cryptographic checksum for said set of said data segments independently of cryptographic checksums calculated for other sets of said data segments (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

24. **Regarding claim 26:** Wee discloses a forwarder for forwarding said packets to a destination (page 1-2 §2).

25. **Regarding claim 27:** Wee discloses a method for ensuring integrity of data, comprising:

receiving a data packet comprising an amount of data partitioned into a plurality of data segments (page 1 col. 1 ¶2).

Wee does not disclose calculating a cryptographic checksum for a first of said plurality of data segments; or enabling said cryptographic checksum for said first of said plurality of data segments to be transmitted separately from said data packet.

Miller discloses calculating a cryptographic checksum for a first of said plurality of data segments (col. 1 lines 27-44); and enabling said cryptographic checksum for said first of said plurality of data segments to be transmitted separately from said data packet (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

26. **Regarding claim 28:** Wee discloses said first data segment and a second of said plurality of data segments (page 3 col. 1 ¶2). Wee does not disclose calculating cryptographic checksums. Miller discloses calculating cryptographic checksums (col. 1 lines 27-44).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

27. **Regarding claim 29:** Wee discloses a method for ensuring integrity of data, comprising: receiving a data packet comprising an amount of data partitioned into at least one data segment (page 1 col. 1 ¶2).

Wee does not disclose calculating a cryptographic checksum for said at least one data segment; or enabling said cryptographic checksum for said at least one data segment to be transmitted separately from said data packet.

Miller discloses calculating a cryptographic checksum for said at least one data segment (col. 1 lines 27-44); and enabling said cryptographic checksum for said at least one data segment to be transmitted separately from said data packet. (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

28. **Regarding claim 30:** Wee does not disclose calculating a second cryptographic checksum for a second of said at least one data segment; and enabling said cryptographic checksum for said at least one data segment to be transmitted separately from said data packet.

Miller discloses calculating a second cryptographic checksum for a second of said at least one data segment (col. 1 lines 27-44); and enabling said cryptographic checksum for said at least one data segment to be transmitted separately from said data packet (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

29. **Regarding claim 32:** Wee discloses an apparatus for verifying the integrity of data, comprising: a receiver, said receiver configured to receive data and a previously determined cryptographic checksum corresponding to said data (page 1 col. 1 ¶2).

Wee does not disclose an integrity check module coupled to said receiver, said integrity check module configured to calculate a new cryptographic checksum corresponding to said received data and to determine whether said new cryptographic checksum matches said previously determined cryptographic checksum.

Miller discloses an integrity check module coupled to said receiver, said integrity check module configured to calculate a new cryptographic checksum corresponding to said received data and to determine whether said new cryptographic checksum matches said previously determined cryptographic checksum (col. 1 lines 27-44).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

30. **Regarding claim 33:** Wee does not disclose that said integrity check module is integral with said receiver. Miller discloses that said integrity check module is integral with said receiver (col. 1 lines 27-44).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

31. **Regarding claim 34:** Wee does not disclose an output coupled to said integrity check module, said output configured to provide an indication of whether said new cryptographic checksum matches said previously determined cryptographic checksum.

Miller discloses an output coupled to said integrity check module, said output configured to provide an indication of whether said new cryptographic checksum matches said previously determined cryptographic checksum (col. 1 lines 27-44).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

32. **Claims 3, 4, 11, 14-22, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wee in view of Miller and further in view of Doyle et al., U.S. Patent Publication No. 2002/0095586 A1 (hereinafter Doyle).**

33. **Regarding claim 14:** The combination of Wee and Miller discloses a method for ensuring the integrity of data, comprising: for a plurality of data packets comprising a plurality of first data segments and a plurality of second data segments, calculating a cryptographic checksum for said plurality of said first data segments; and enabling said cryptographic checksum for said plurality of said first data segments to be transmitted separately from said plurality of said data packets, as indicated regarding claim 1, above.

Neither Wee nor Miller discloses a computer readable medium having instructions stored therein for implementing said method. Doyle discloses a computer readable medium having instructions stored therein for implementing said method (Abstract).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to implement the combination Wee and Miller via the technique taught by Doyle in order to conveniently and economically distribute operational copies of the software embodying the method to multiple computing devices (*see* Doyle [0018]).

34. **Regarding claims 3, 16 and 31:** The combination of Wee and Miller, as indicated regarding claims 1, 14 and 29, above, does not disclose including said first cryptographic checksum for said plurality of said first data segments and said cryptographic checksum for said plurality of said second data segments in the same data packet.

Doyle discloses including said first cryptographic checksum for said plurality of said first data segments and said cryptographic checksum for said plurality of said second data segments in the same data packet [0069].

Therefore, it would have been obvious to one skilled in the art at the time of the invention to implement the combination Wee and Miller via the technique taught by Doyle in order to create a more computationally efficient data verification system (*see* Doyle [0018] and Miller col. 2 lines 5-14).

35. **Regarding claims 4 and 17:** The combination of Wee and Miller, as indicated regarding claims 1, 14 and 29, above, does not disclose that said cryptographic checksum for said plurality of said first data segments is calculated at a rate which is different from the rate at which said cryptographic checksum for said plurality of said second data segments is calculated.

Doyle discloses that said cryptographic checksum for said plurality of said first data segments is calculated at a rate which is different from the rate at which said cryptographic checksum for said plurality of said second data segments is calculated [0073]-[0075].

Therefore, it would have been obvious to one skilled in the art at the time of the invention to implement the combination Wee and Miller via the technique taught by Doyle in order to

create a more computationally efficient data verification system (*see* Doyle [0018] and Miller col. 2 lines 5-14).

36. **Regarding claims 11 and 20:** The combination of Wee and Miller, as indicated regarding claims 1 and 14, above, does not disclose that said data is stored in a storage medium. Doyle discloses that said data is stored in a storage medium [0003] and [0005].

Therefore, it would have been obvious to one skilled in the art at the time of the invention to implement the combination Wee and Miller via the technique taught by Doyle in order to create a more computationally efficient data verification system (*see* Doyle [0018] and Miller col. 2 lines 5-14).

37. **Claim 15** is rejected for the same reason as indicated regarding claim 2, above.

38. **Claim 18** is rejected for the same reason as indicated regarding claim 7, above.

39. **Claim 19** is rejected for the same reason as indicated regarding claim 10, above.

40. **Claim 21** is rejected for the same reason as indicated regarding claim 12, above.

41. **Claim 22** is rejected for the same reason as indicated regarding claim 13, above.

Conclusion

2. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is:

- Brunk et al., U.S. Patent Publication No. 2002/0157005 A1 regarding including a metric in a digital watermark for media authentication.

- Walmsley et al., U.S. Patent Publication No. 2003/0159036 A1 regarding a validation protocol and system.
- Ramage, U.S. Patent No. 4,790,028 regarding a method for generating variably scaled displays.
- Mumford, U.S. Patent No. 5,321,807 regarding an accelerated graphics display method.
- Sciammarella et al., U.S. Patent No. US 6,320,599 B1 regarding a zooming scale indicator in computer graphics.
- Romrell, U.S. Patent No. 6,396,805 B2 regarding a system for recovering from disruption of a data transfer.
- Mualem et al., U.S. Patent Publication No. 2002/0166070 A1 regarding reducing errors of a security association.
- Shanklin et al., U.S. Patent No. 6,954,775 B1 regarding parallel intrusion detection sensors with load balancing for high speed networks.
- Feldbau et al., U.S. Patent No. 6,571,334 B1 regarding authenticating the dispatch and contents of documents.
- Sudia, U.S. Patent No. 5,850,451 regarding an enhanced cryptographic system with key escrow feature.
- Benayoun et al., U.S. Patent No. 6,804,257 B1 regarding framing and protecting variable length packet streams.
- Wee et al., U.S. Patent Publication No. 2002/0163911 A1 regarding midstream transcoding of secure scalable packets in response to downstream requirements.

Please direct any inquiry concerning this communication or earlier communications from the examiner to Bea Koempel-Thomas whose telephone number is 571-270-1252. The examiner can normally be reached on Monday - Thursday & alternate Fridays; 0730 - 1700.

If attempts to reach the examiner by telephone are unsuccessful, please contact the examiner's supervisor, Gilberto Barron, at 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Bea Koempel-Thomas, Esq.
Patent Examiner
AU 2132

1/31/2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100